PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-326696
(43)Date of publication of application : 22.11.2001

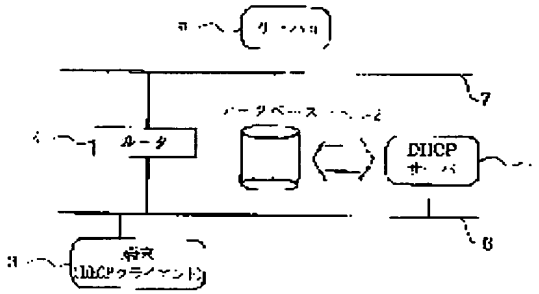
(51)Int.Cl. H04L 12/66
G06F 13/00
H04L 12/46
H04L 12/28
H04L 12/56

(21)Application number : 2000-146598
(22)Date of filing : 18.05.2000

(71)Applicant : NEC CORP
(72)Inventor : KASHIMA KENICHI

(54) METHOD FOR CONTROLLING ACCESS

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an access control method to a server in the unit of users by utilizing a DHCP in a network consisting of terminals connected to a sub net and application servers connected to the server via routers.
SOLUTION: When a terminal is connected to a network, the terminal broadcasts connection request information, the server broadcasts a proposal of assigned setting information, the terminal receiving the proposal of the assigned setting information broadcasts request information including information required for authentication, the server receives information required for the authentication are references a database connected to the server to authenticate the terminal. If the authentication is successful, the server requests access control, corresponding to the terminal to the route. The router, receiving the request, executes filtering of a transmission reception packet on the basis of various sets of information included in the request. The router transmits result information to the terminal and to the server, on the basis of the result of filtering of the transmission reception packet, to complete the connection between the terminal and the server.



LEGAL STATUS

[Date of request for examination] 13.04.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－326696
（P2001－326696A）
(43)公開日　平成13年11月22日(2001.11.22)

(51)Int.Cl.[7]		識別記号	Ｆ Ｉ		テーマコード(参考)
Ｈ０４Ｌ	12/66		Ｇ０６Ｆ	13/00	３５１Ｚ　５Ｂ０８９
Ｇ０６Ｆ	13/00	３５１	Ｈ０４Ｌ	11/20	Ｂ　５Ｋ０３０
Ｈ０４Ｌ	12/46			11/00	３１０Ｃ　５Ｋ０３３
	12/28			11/20	１０２Ｄ
	12/56				

審査請求　有　請求項の数７　ＯＬ　（全 ８ 頁）

(21)出願番号　特願2000－146598(P2000－146598)

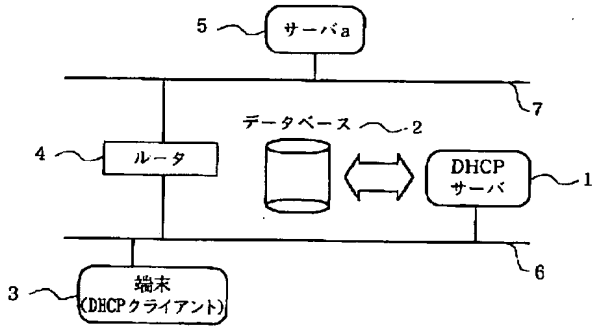
(22)出願日　平成12年５月18日(2000.5.18)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　鹿島　謙一
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100088328
弁理士　金田　暢之　（外２名）

最終頁に続く

(54)【発明の名称】　アクセス制御方法

(57)【要約】
【課題】　サブネットに接続されている端末とサーバとルータを介して接続しているアプリケーションサーバから構成されるネットワークでＤＨＣＰを利用してユーザ単位でのサーバへのアクセス制御方法を提供する。
【解決手段】　端末がネットワークに接続する際に、接続要求情報をブロードキャストし、サーバが割り当て設定情報の提案をブロードキャストし、割り当て設定情報の提案を受けた端末が認証に要する情報を含む要求情報をブロードキャストし、サーバが認証に要する情報を受け、サーバに接続されているデータベースを参照して認証する。認証に成功すればサーバが端末に対応するアクセス制御をルータに依頼する。依頼を受けたルータは依頼に含まれる各種情報を基に送受パケットのフィルタリングを実施する。ルータは送受パケットのフィルタリングの結果に基づき端末とサーバに結果情報を送信し、端末とサーバの接続を完了する。



1

【特許請求の範囲】

【請求項１】　第１サブネットに接続されているＤＨＣＰクライアント端末と、データベースを持つＤＨＣＰサーバと、第１サブネットとルータを介して接続される第２サブネットと、第２サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法において、

ＤＨＣＰを利用し、認証情報データベースによってユーザ単位での前記クライアント端末を認証し、クライアント端末の送受パケットをサーバとルータの連携によってフィルタリングすることを特徴とするアクセス制御方法。

【請求項２】　第１サブネットに接続されているＤＨＣＰクライアント端末と、データベースを持つＤＨＣＰサーバと、第１サブネットとルータを介して接続される第２サブネットと、第２サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法であって、

前記クライアント端末が、ネットワークに接続する際に、ＤＨＣＰサーバから端末認証とユーザ認証を得るステップと、

前記認証によって得られる情報を基にＤＨＣＰサーバとルータが連携してユーザ単位のアクセス制御を実施するステップと、

前記認証を得たＤＨＣＰクライアント端末のネットワーク接続が完了するステップを有するアクセス制御方法。

【請求項３】　第１サブネットに接続されているＤＨＣＰクライアント端末と、データベースを持つＤＨＣＰサーバと、第１サブネットとルータを介して接続される第２サブネットと、第２サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法であって、

前記ＤＨＣＰクライアント端末が前記ネットワークに接続する際に、前記ＤＨＣＰクライアント端末が接続要求情報をブロードキャストし、前記ＤＨＣＰサーバが割り当て設定情報の提案をブロードキャストするステップと、

割り当て設定情報の提案を受けた前記ＤＨＣＰクライアント端末が認証に要する情報を含むＤＨＣＰ要求情報をブロードキャストし、ＤＨＣＰサーバが前記ＤＨＣＰクライアント端末の認証に要する情報を受け、ＤＨＣＰサーバに接続されているデータベースを参照して認証するステップと、

認証に成功すればＤＨＣＰサーバが前記ＤＨＣＰクライアント端末に対応するアクセス制御をルータに依頼し、認証に失敗すれば前記ＤＨＣＰクライアント端末に失敗を報告するステップと、

依頼を受けたルータは依頼に含まれる各種情報を基に送受パケットのフィルタリングを設定するステップと、

前記ルータは送受パケットのフィルタリングの設定結果

2

に基づき前記ＤＨＣＰサーバに結果情報を送信し、さらに前記ＤＨＣＰサーバが前記ＤＨＣＰクライアント端末に結果情報を返し、最終的に前記ＤＨＣＰクライアント端末がネットワーク接続が完了するステップを有するアクセス制御方法。

【請求項４】　前記送受パケットのフィルタリングを実施するステップが、

前記ルータが、前記ＤＨＣＰクライアント端末から送信されるすべてのパケットを受信するステップと、

前記ルータが、前記ＤＨＣＰサーバで設定されたアクセスリストに基づいて、前記パケットが許可されたものであればアプリケーションサーバに転送し、不許可ならばアプリケーションサーバに転送せずにパケットを廃棄し、履歴としてログ情報を残すフィルタリングステップを有する請求項１乃至３の何れかに記載のアクセス制御方法。

【請求項５】　前記第１サブネットに接続されているＤＨＣＰクライアント端末が、

特別なサブネットマスクを設定して、前記ルータと前記ＤＨＣＰクライアント端末のみの第３サブネットを形成するステップと、

前記第１サブネットに接続されているアプリケーションサーバに前記ルータを介してパケットの送受信を行うステップを有する請求項１乃至４の何れかに記載のアクセス制御方法。

【請求項６】　前記第１サブネットにさらにエージェント端末を接続し、前記エージェント端末が、

ネットワークに流れるＩＰおよびＭＡＣアドレス情報を前記エージェント端末の持つデータベースに収集するステップと、

前記ＤＨＣＰサーバが持つ前記ＤＨＣＰクライアント端末に関するキャッシュデータと前記エージェント端末のデータベースとを比較検証するステップを有する請求項１乃至４の何れかに記載のアクセス制御方法。

【請求項７】　第１サブネットに接続されているＤＨＣＰクライアント端末と、データベースを持つＤＨＣＰサーバと、第１サブネットとルータを介して接続される第２サブネットと、第２サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法において、

前記ＤＨＣＰクライアント端末毎にアプリケーションサーバへのアクセス制御が行うステップと、

前記ＤＨＣＰサーバによるユーザ認証だけではなく、ＤＨＣＰサーバとルータが連携して、アクセス制御を行うステップと、

前記ＤＨＣＰクライアント端末とルータのみのサブネットを構築するステップと、

第１サブネットに接続するエージェント端末により不正接続の端末を検出するステップを有することを特徴とするアクセス制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は端末をネットワークに接続する際のアクセス制御方法に関し、特に動的ホスト設定プロトコル（Ｄｙｎａｍｉｃ　Ｈｏｓｔ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ、以降ＤＨＣＰと称す）を利用するユーザ単位でのサーバへのアクセス制御に関する。

【０００２】

【従来の技術】端末をネットワークに接続する際に、ＤＨＣＰは非常に有用なプロトコルである。しかし、ＤＨＣＰを使用しても運用面でセキュリティ上に問題点がある。

【０００３】

【発明が解決しようとする課題】第１の問題点は、接続要求があれば如何なる端末に対してもインターネットプロトコル（以降、ＩＰと称す）アドレスを割り当て、ネットワークへの接続を許可してしまうということである。その理由は、ＤＨＣＰには認証の概念が存在しないためである。

【０００４】第２の問題点は、運用上ある端末あるいはユーザに対して、特定サーバへのアクセスを拒否したい場合に、それを実現ができないことである。

【０００５】ＤＨＣＰによりＩＰアドレスを割り当てられた端末は、ネットワークを通じて、ＷＷＷ、メール、Ｎｅｗｓ、プリンタ、ファイルなどのサービスを行っているアプリケーションサーバへアクセスすることが可能となる。もし特定アプリケーションサーバへのアクセスを拒否したい場合には、ネットワークへの接続そのものを拒否する必要があり、ユーザの利便性を著しく損なうことになっている。

【０００６】第３の問題点は、何らかの方法で、ネットワークのＩＰアドレスを不正入手し、手動設定を行うことによりネットワーク接続した場合には、それを防止することができないことである。

【０００７】本発明の目的は、以上の問題点を解決するような、サブネットに接続されているＤＨＣＰクライアント端末とＤＨＣＰサーバとルータを介して接続しているアプリケーションサーバから構成されるネットワークでＤＨＣＰを利用してユーザ単位でのアプリケーションサーバへのアクセス制御方法を提供することである。

【０００８】

【課題を解決するための手段】本発明のアクセス制御方法は、第１サブネットに接続されているＤＨＣＰクライアント端末と、データベースを持つＤＨＣＰサーバと、第１サブネットとルータを介して接続される第２サブネットと、第２サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法において、ＤＨＣＰを利用し、認証情報データベースによってユーザ単位でのクライアント端末を認証し、クライアント端末の送受パケットをサーバとルータの協同によってフィルタリングすることを特徴とする。

【０００９】また、本発明のアクセス制御方法は、第１サブネットに接続されているＤＨＣＰクライアント端末と、データベースを持つＤＨＣＰサーバと、第１サブネットとルータを介して接続される第２サブネットと、第２サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法であって、クライアント端末が、ネットワークに接続する際に、ＤＨＣＰサーバから端末認証とユーザ認証を得るステップと、認証によって得られる情報を基にＤＨＣＰサーバとルータが連携してユーザ単位のアクセス制御を実施するステップと、アクセスされたクライアント端末のネットワークへの接続が完了するステップを有する。

【００１０】さらに、本発明のアクセス制御方法は、第１サブネットに接続されているＤＨＣＰクライアント端末と、データベースを持つＤＨＣＰサーバと、第１サブネットとルータを介して接続される第２サブネットと、第２サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法であって、ＤＨＣＰクライアント端末がネットワークに接続する際に、ＤＨＣＰクライアント端末が接続要求情報をブロードキャストし、ＤＨＣＰサーバが割り当て設定情報の提案をブロードキャストするステップと、割り当て設定情報の提案を受けたＤＨＣＰクライアント端末が認証に要する情報を含むＤＨＣＰ要求情報をブロードキャストし、ＤＨＣＰサーバがＤＨＣＰクライアント端末の認証に要する情報を受け、ＤＨＣＰサーバに接続されているデータベースを参照して認証するステップと、認証に成功すればＤＨＣＰサーバがＤＨＣＰクライアント端末に対応するアクセス制御をルータに依頼し、認証に失敗すればＤＨＣＰクライアント端末に失敗を報告するステップと、依頼を受けたルータは依頼に含まれる各種情報を基に送受パケットのフィルタリングの設定を行うステップと、ルータは送受パケットのフィルタリングの設定結果に基づきＤＨＣＰサーバに結果情報を送信し、さらに前記ＤＨＣＰサーバが前記ＤＨＣＰクライアント端末に結果情報を返し、最終的に前記ＤＨＣＰクライアント端末のネットワーク接続が完了するステップを有する。

【００１１】また、送受パケットのフィルタリングを実施するステップが、ルータが、ＤＨＣＰクライアント端末から送信されるすべてのパケットを受信するステップと、ルータが、ＤＨＣＰサーバで設定されたアクセスリストに基づいて、パケットが許可されたものであればアプリケーションサーバに転送し、不許可ならばアプリケーションサーバに転送せずにパケットを廃棄し、履歴としてログ情報を残すフィルタリングステップを有する。

5

【００１２】また、第１サブネットに接続されているＤＨＣＰクライアント端末は、特別なサブネットマスクを設定して、ルータとＤＨＣＰクライアント端末のみの第３サブネットを形成するステップと、第１サブネットに接続されているアプリケーションサーバにルータを介してパケットの送受信を行うステップを有する。

【００１３】また、第１サブネットにさらにエージェント端末を接続し、エージェント端末は、ネットワークに流れるＩＰおよび媒体アクセス制御（以下ＭＡＣと称す）アドレス情報をエージェント端末の持つデータベースに収集するステップと、ＤＨＣＰサーバが持つＤＨＣＰクライアント端末のキャッシュデータとエージェント端末のデータベースとを比較検証するステップを有する。

【００１４】さらに、本発明のアクセス制御方法は、第１サブネットに接続されているＤＨＣＰクライアント端末と、データベースを持つＤＨＣＰサーバと、第１サブネットとルータを介して接続される第２サブネットと、第２サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法において、ＤＨＣＰクライアント端末毎にアプリケーションサーバへのアクセス制御が行うステップと、ＤＨＣＰサーバによるユーザ認証だけではなく、ＤＨＣＰサーバとルータが連携して、アクセス制御を行うステップと、ＤＨＣＰクライアント端末とルータのみのサブネットを構築するステップと、第１サブネットに接続するエージェント端末により不正接続の端末を検出するステップを有することを特徴とする。

【００１５】

【発明の実施の形態】次に本発明の実施の形態について図面を参照して詳細に説明する。

【００１６】図１を参照すると、本発明の実施例は、ＤＨＣＰサーバ１と、データベース２と、端末３（ＤＨＣＰクライアント）と、ルータ４と、端末３と別のサブネット７上に存在するサーバａ５とから構成される。

【００１７】ＤＨＣＰサーバ１は、通常のＤＨＣＰサーバに加えて、ユーザ認証用のデータとユーザアクセス制御用のデータを含むデータベース２を有す。ＤＨＣＰサーバ１は、端末３からの要求に対して認証を行い、ルータ４に対してユーザに対応したアクセス制御を依頼する。

【００１８】データベース２は、認証データとキャッシュデータから成る。認証データは、認証に必要なユーザＩＤ、パスワード、ユーザに対応したアクセス制御を行うためのアクセスリストを含む。アクセスリストは、発信元ＩＰアドレス（割り当て予定アドレス）、宛先ＩＰアドレス（各種サーバのＩＰアドレス、ネットワークアドレス）、発信元ポート番号（任意）、宛先ポート番号（各種サーバのポート番号）などのパラメータを組み合わせて、パケットの転送許可、不許可を記述したものである。

6

【００１９】また、キャッシュデータは、運用中に動的に変化するデータで、ユーザＩＤとそのユーザに割り当てたＩＰアドレス、ユーザの使用している端末のＭＡＣアドレス（Ｅｔｈｅｒｎｅｔ（登録商標）アドレス）、ＩＰアドレスを割り当てた時刻、リース時間などを含む。

【００２０】端末３は、ＤＨＣＰサーバ１に対してＩＰアドレスなどの設定情報の割り当てを要求するとともに、認証を受けるための認証情報を提供する。ルータ４は、ＤＨＣＰサーバ１からの依頼を受けて、アクセス制御を行う。端末３宛てのパケットは必ずこのルータ４を経由することになる。サーバａ５は、ＷＷＷ、メール、Ｎｅｗｓ、ファイル、プリンタなどの種々のサービスを提供している端末を示し、端末３と別サブネット７上に存在する。

【００２１】次に、図１及び図２及び図３を参照して本実施例の動作について詳細に説明する。

【００２２】まず最初に、端末３がネットワークへ接続する際の、認証手順を含んだＩＰアドレス割り当ての手順を図２を参照して説明する。

【００２３】端末３は、ＤＨＣＰＤＩＳＣＯＶＥＲをブロードキャストする（ステップ２０）。ＤＨＣＰＤＩＳＣＯＶＥＲを受信したＤＨＣＰサーバ１は、割り当てるべき設定情報を提案するために、ＤＨＣＰＯＦＦＥＲをブロードキャストする（ステップ２１）。ここまでは通常のＤＨＣＰのフローと同様である。設定情報の提案を受けた端末３は、ＤＨＣＰＲＥＱＵＥＳＴをＤＨＣＰサーバ１へブロードキャストする（ステップ２２）。このメッセージには、ユーザＩＤ、パスワードオプション（ハッシュ化し不可視化する）が含まれる。

【００２４】端末３からユーザＩＤ、パスワードを含むＤＨＣＰＲＥＱＵＥＳＴを受信したＤＨＣＰサーバ１は、端末認証およびユーザ認証を行う（ステップ２３）。端末認証は、端末３から送信されてきたＭＡＣアドレスを検索キーとして、データベース２を参照することによって行われる。次に、端末３から送信されてきたユーザＩＤ、パスワードからデータベース２を参照してユーザ認証が行われる。認証に成功すれば、ＤＨＣＰサーバ１はユーザに対応したアクセス制御をルータ４へ依頼するためにＣｏｎｆｉｇｕｒｅ－Ｒｅｑｕｅｓｔを送信する（ステップ２４）。認証に失敗したならば、クライアントへＤＨＣＰＮＡＫを送信する。

【００２５】ＤＨＣＰサーバ１から送信されるＣｏｎｆｉｇｕｒｅ－Ｒｅｑｕｅｓｔには、アクセスリスト、端末３のＭＡＣアドレス、割り当て予定のＩＰアドレスといった情報が含まれる。

【００２６】ルータ４は、ＤＨＣＰサーバ１から依頼されたアクセスリストに基づき、適当なパケットフィルタの設定を行う（ステップ２５）。設定が完了したら、ル

ータ４はＣｏｎｆｉｇｕｒｅ－ＡｃｋをＤＨＣＰサーバ１へ送信する（ステップ２６）。ルータ４から、アクセス制御の設定完了のＣｏｎｆｉｇｕｒｅ－Ａｃｋを受信したら、ＤＨＣＰサーバ１は端末３に対してＤＨＣＰＡＣＫを送信する（ステップ２７）。以上で、ユーザ認証を経て、ネットワークを接続するための必要最低限の設定すなわち初期化が完了となる（ステップ２８）。

【００２７】この時点で、端末３は、ユーザ認証を経て、最低限の設定情報として、ＩＰアドレス、サブネットマスク、ルーティング情報（デフォルトルート）、ＩＰアドレスのリース時間が既に設定されており、ルータにはアクセスリストの設定が行われている。

【００２８】次に、端末３（ＤＨＣＰクライアント）とそれと別サブネット７上に存在するサーバａ５間のデータ通信の流れを追いながら、アクセス制御がどのように実現されているのかを説明する。

【００２９】端末３は、ルーティングテーブルに基づき、サーバａ５宛てのパケットをルータへ送信する。それを受信したルータ４は、ルーティングテーブルに基づき、そのパケットをサーバａ５へ転送する。こうしてサーバａ５は、端末３から送信されたパケットを受信することができる。逆に、サーバａ５から端末３宛のパケットは、そのルーティングテーブルに基づき、ルータ４へ送られる。それを受信したルータ４は、そのルーティングテーブルに基づき、端末３へパケットを転送する。こうして端末３は、サーバａ５から送信されたパケットを受信することができる。

【００３０】上述のように、端末３から送信されるすべてのパケットは必ずルータ４を経由することになる。つまり、ルータ４は送信パケットが許可されたものであれば転送し、不許可ならば転送せずにパケットを廃棄し、その旨のログ情報を残す。それゆえ、ルータ４はステップ２５で設定したアクセスリストに基づいて、アクセス制御が可能となる。

【００３１】最後に、端末３がすべての処理を終了して、ネットワークから切り離される際に、ＩＰアドレスを開放する手順を図３を用いて説明する。

【００３２】端末３は、ＤＨＣＰサーバ１に対してＤＨＣＰＲＥＬＥＡＳＥを送信する（ステップ３１）。このメッセージには、ユーザＩＤ、パスワードオプションが含まれる。ＤＨＣＰＲＥＬＥＡＳＥを受信したＤＨＣＰサーバ１は、そのメッセージに含まれるユーザＩＤ、パスワードからデータベース２に基づいて認証を行なう（ステップ３２）。認証に成功すれば、ユーザに対応したアクセス制御の解除をルータ４へ依頼する。そのために、ＤＨＣＰサーバ１はＴｅｒｍｉｎａｔｅ－Ｒｅｑｕｅｓｔをルータ４へ送信する（ステップ３３）。Ｔｅｒｍｉｎａｔｅ－Ｒｅｑｕｅｓｔを受信したルータ４は、ＤＨＣＰサーバ１から依頼されたアクセスリストに基づき設定を解除し、Ｔｅｒｍｉｎａｔｅ－ＡｃｋをＤＨＣＰサーバへ送信する（ステップ３４）。

【００３３】次に本発明の第２の実施例について図面を参照して詳細に説明する。図４によると、本実施例は、端末３と物理的に同一のサブネット６上にあるサーバｂ８に対するアクセス制御という点が先の実施例と異なる。

【００３４】端末３は、図２の手順で、ユーザ認証を経て、ＤＨＣＰサーバ１が割り当てる最低限の設定情報として、ＩＰアドレス、サブネットマスク（２５５．２５５．２５５．２５１）、ルーティング情報（デフォルトルート）、ＩＰアドレスのリース時間が割り当てられる。さらに、最初の実施例では実施されなかった端末３自身のＡＲＰ　Ｒｅｐｌｙの停止が追加実行される。

【００３５】ルータ４には、アクセスリストの設定、端末３に対するＰｒｏｘｙ　ＡＲＰの設定、端末３のＭＡＣアドレスのＡＲＰテーブルへの登録が図２のステップ２５の時点で行われる。Ｐｒｏｘｙ　ＡＲＰとは、端末３のＩＰアドレスのＡＲＰＲｅｑｕｅｓｔに対して、ルータ４が代わりにＡＲＰ　Ｒｅｐｌｙを応答するものである。

【００３６】ここで特徴的なのは、サブネットマスクとして２５５．２５５．２５５．２５１、３０ビットマスクを使用していることである。この設定により、図４に示すように、ルータ４と端末３は、所属端末が２つのみのサブネット９を形成することになる。そのためサーバｂ８は、たとえ物理的には同一サブネットに存在しても、論理的に別サブネット上に存在していることになり、サーバｂ８宛てのパケットはルータ４を経由して送信される。

【００３７】次にサーバｂ８と端末３の通信手順を図５、図６を参照して詳細に説明する。

【００３８】図５によれば、まず、端末３はＡＲＰ　Ｒｅｑｕｅｓｔをブロードキャストして、ルータ４のＭＡＣアドレスを問い合わせる（ステップ４０）。ＡＲＰ　Ｒｅｑｕｅｓｔを受信したルータ４は、ＡＲＰ　Ｒｅｐｌｙで応答する（ステップ４１）。ルータ４のＭＡＣアドレスを解決した端末３は、ルータ４へサーバｂ８宛てのパケットを送信する（ステップ４２）。それを受信したルータ４は、ルーティングを行い、パケットをサーバｂ８へ転送しようとする。（ステップ４３）。そこで、ルータ４はＡＲＰ　Ｒｅｑｕｅｓｔをブロードキャストして、サーバｂ８のＭＡＣアドレスを解決しようとする（ステップ４４）。それに対してサーバｂ８はＡＲＰ　Ｒｅｐｌｙで応答する（ステップ４５）。それを受信したルータ４は、サーバｂ８へサーバｂ８宛てのパケットを転送する（ステップ４６）。このとき、サーバｂ６宛てのパケットはルータ４を経由している。

【００３９】逆に、サーバｂ８から端末３宛てのパケットの送信の手順を説明する。図６によれば、サーバｂ８は、ＡＲＰ　Ｒｅｑｕｅｓｔをブロードキャストして、

端末３のＭＡＣアドレスを解決しようとする（ステップ５０）。それに対して、Ｐｒｏｘｙ　ＡＲＰの設定がされている（ステップ５１）ルータ４は、ＡＲＰ　Ｒｅｐｌｙに自身のＭＡＣアドレスを入れて応答する（ステップ５２）。一方、端末３は、ＡＲＰ　Ｒｅｐｌｙ停止５３を行っているので、このＡＲＰ　Ｒｅｑｕｅｓｔには応答することができない。アドレス解決をしたサーバｂ８は、ルータ４へ端末３宛てのパケットを送信する（ステップ５４）。それを受信したルータ４は、ルーティングを行い（ステップ５５）、端末３へ端末３宛てのパケットを転送する（ステップ５６）。このとき、ＡＲＰテーブルには端末３のＩＰアドレスとＭＡＣアドレスの組が登録されているので、ＡＲＰを使うことなく、ユニキャストでパケットを転送することができる。

【００４０】いずれの場合も、端末３から送信されるすべてパケットは、必ずルータ４を経由することになるので、ルータ４のアクセスリストによりアクセス制御が可能となる。

【００４１】以上、サーバが端末３と同一サブネット６に存在する場合のアクセス制御方法を説明したが、サーバが端末３と同一サブネット６と別サブネット７に同時に存在する場合でも、本実施例と同様にアクセス制御が可能である。

【００４２】次に本発明の第３の実施例について図面を参照して詳細に説明する。図７によると、本実施例は、Ｅｔｈｅｒｎｅｔ上に流れるＡＲＰ　Ｒｅｐｌｙパケットをキャプチャーし、ＩＰアドレスとＭＡＣアドレスの組をデータベースに保持する機能を持つエージェント７０が存在する点が異なる。

【００４３】本実施例では、先の実施例を運用中に、何らかの方法でＩＰアドレスを不正入手し、手動設定を行うことによりネットワークに端末に接続した場合の対策方法について説明する。

【００４４】図８において、エージェント７０は、Ｅｔｈｅｒｎｅｔ上に流れるＡＲＰ　ＲｅｐｌｙパケットをキャプチャーしてＩＰアドレスとＭＡＣアドレスの組を収集し、それをデータベース８０に保持する。

【００４５】一方、ＤＨＣＰサーバ１が持つデータベース２には、現在アドレスが割り当てられているユーザＩＤとそのユーザに割り当てたＩＰアドレス、ユーザの使用している端末のＭＡＣアドレス、ＩＰアドレスを割り当てた時刻、リース時間などを含む。

【００４６】ＤＨＣＰ以外の手順で正規にＩＰアドレスを割り当てられた端末の情報を加えたキャッシュデータ２と、エージェントのデータベース８０とを定期的に比較検証する。もし、不正に入手したＩＰアドレスを使用していた端末が存在すると、キャッシュデータにはその端末の情報が存在しないため、上記の比較検証によって不正接続を検出することができる。

【００４７】本実施例では、エージェントの導入により、ＩＰアドレスの不正入手による接続を検出できるという新たな効果を有する。

【００４８】

【発明の効果】第１の効果は、ユーザ及び端末毎にネットワーク接続可否を制御することができることにある。

【００４９】その理由は、ＤＨＣＰにユーザ認証を導入したからである。

【００５０】第２の効果は、ユーザ及び端末毎にアプリケーションサーバへのアクセス制御を行うことができることにある。

【００５１】その理由は、ＤＨＣＰサーバとルータが連携してパケットフィルタを設定し、さらに端末から送信されるすべてのパケットがルータを通過するようにしたためである。

【００５２】第３の効果は、ネットワークのＩＰアドレスを不正入手し、手動設定を行うことによりネットワーク接続した端末を検出することができることにある。

【００５３】その理由は、ＩＰアドレスとＭＡＣアドレスの組を収集する機能を持つエージェントを導入したためである。

【００５４】第４の効果は、サーバ個別のアクセス制御を不要とすることができることにある。

【００５５】その理由は、端末の接続段階でアクセス制御を行い、端末からサーバ宛てのパケットが一切届かないからである。

【図面の簡単な説明】

【図１】第１の実施例の構成を示すネットワーク図である。

【図２】第１の実施例の動作を示すシーケンス図である。

【図３】第１の実施例の動作を示すシーケンス図である。

【図４】第２の実施例の構成を示すネットワーク図である。

【図５】第２の実施例の動作を示すシーケンス図である。

【図６】第２の実施例の動作を示すシーケンス図である。

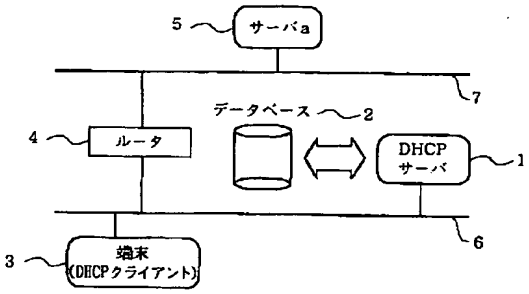
【図７】第３の実施例の構成を示すネットワーク図である。

【図８】第３の実施例の動作を示す図である。

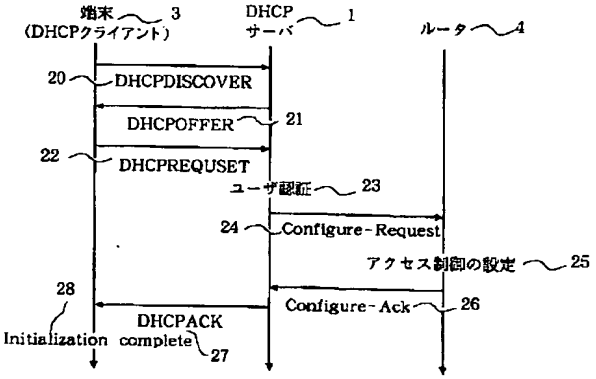
【符号の説明】

１　　ＤＨＣＰサーバ
２　　データベース
３　　端末（ＤＨＣＰクライアント）
４　　ルータ
５　　サーバａ
６、７、９　　サブネット
８　　サーバｂ
７０　　エージェント

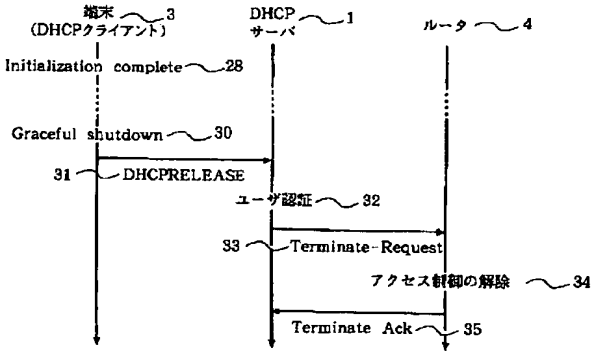
【図１】



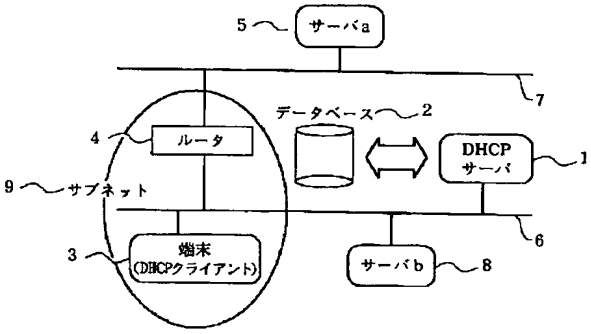
【図２】



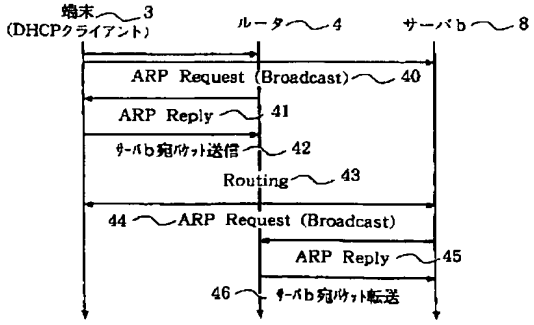
【図３】



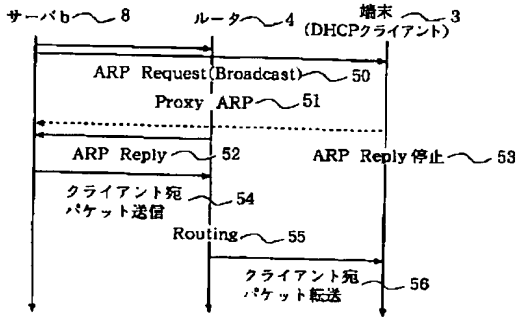
【図４】



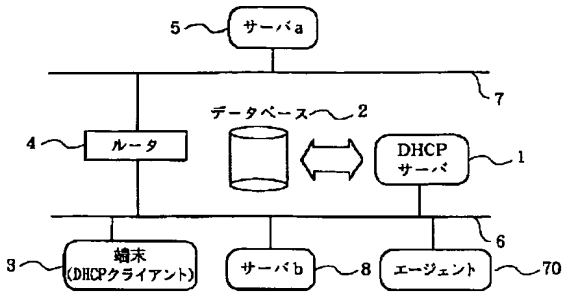
【図５】



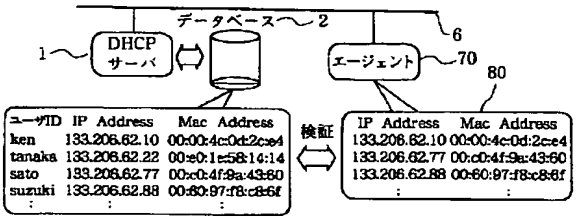
【図６】



【図７】



【図８】



フロントページの続き

Ｆターム(参考) 5B089 GA11 GA21 GA31 HA01 HA06
HA10 HB18 JB00 KB06 KB13
KC58 MB01
5K030 GA15 HA08 HC14 HD03 HD07
HD09 JT03 JT06 KA05 LB02
LC13 LD19 LD20 MD09
5K033 AA08 CB01 CB08 CC01 DA01
DA05 DB19 DB20 EA07 EC03